TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI
VICTORIA
UNIVERSITY OF WELLINGTON

EXAMINATIONS — 2009
END-YEAR

COMP306

Computer Networks

Time allowed: THREE HOURS

Instructions: The examination contains 6 questions, you must answer all questions

Each question is worth 30 marks.

The exam consists of 180 marks in total.

Paper foreign to English language dictionaries are allowed.

Electronic dictionaries and programmable calculators are not allowed.

Question 1 Cryptography & Cryptanalysis **[30 marks]**

(a) [2 Marks] Both Steganography and Cryptography seek to prevent the content of a message from being revealed. However they both achieve this in very different ways. Explain the significant difference between Steganography and Cryptography, examples should be given to reinforce your explanation.
Boils down to, stegos – to physically hide the message (example microdots), crypt – to conceal the meaning, while the message may be viewed (example enigma). 0.5 Marks ea. def + ex.

(b) [2 Marks] What is Kerckhoffs principle?
"All algorithms must be public; only the keys are secret"

(c) [4 Marks] Show, with the use of an example, how a polyaphabetic cypher might encode the sentence "Adam". You may choose your own scheme and key – so you must explain your scheme, show all steps and information used in the process.
It is the process I am interested in. I would like to see some means for switching alphabets based on character position [2 Marks], and some means of generating the alphabet selection from a short key [2 Marks].

(d) [6 Marks] Is a polyalphabetic cypher susceptable to a frequency analysis attack? Be sure to state any conditions or assumptions your arguement is relying on. Use an example to support your claims.
Well, this is a box of worms to mark… Basically they can argue it is susceptable to frequency analysis as shown by Babbage's cracking of the Vignire Cypher due to the recovery of the length of the key via GCD due to repeated sequences and then treat this as a collection of smaller monoalphabetic cyphers to which frequency analysis might be applied. Or….they might argue that the weakness is in the key and providing a random key the same length as the message is used, then we have a one-time-pad which is uncrackable. I don't mind which answer, as either shows good understanding.

(e) Consider the efforts at Blechly park to crack the WWII German enigma code.

i. [4 Marks] What type of Cypher was the Enigma Code?
It looks like a subsitution cypher rather than transposition cypher, as each encoded letter retains its place in the cyphertext, but its encrypted value relies on the preceeding letters – which makes it a form of product cypher.

ii. [8 Marks] State and explain (with examples were needed) the four techniques used by the Cryptanalyists at Blechly park to crack the Enigma code.
cillies (rules that decreased combinations – girlfriends intials as a day code etc.),
cribs(templates i.e., rigid formating rules, i.e. wetter reports),
pinches(theft of code books etc. via special ops), and
seeding(changing the environment to force and encoded reaction, i.e. laying a minefield in a certain area and then intercepting the message (incl coords) and applying cribs to anal.)
[1 mark each term, 1 mark proper explanation]

(f) [4 Marks] Define what it means for a Cryptographic system to be secure.

When the cryptanalyst manages to cause some text of his/her choice to be encrypted this is known as a ***chosen plaintext attack****. A secure system is secure against* ***chosen plaintext attack****.*

Question 2 Cryptography and Authentication **[30 marks]**

(a) [4 Marks] What is Cypher block chaining, and why was it needed in the DES encryption standard?

Cypher block chaining XORs the result of the current 64 bit block with the previous 64 bit block. Otherwise, the 64 bit blocks can be analysed on their own. Chaining over comes this by making each block depend on all of the proceeding blocks. [2 Marks each]

(b) [8 Marks] The major problem in the 1970s was the exchange of keys. Outline the DHM (diffie, Hellman and Merkle) algorithm for establishing a key, without a prior physical key exchange. Be sure to explain the importance of one-way functions in this protocol. You may explain the algorithm directly or by using an analogy.

Slides 7-9 Lecture 4. I would be happy to see the paint analogy here along with how hard it is to reverse mixed paint. The mathematical treatment is also fine :P This should not be confused with RSA, and they should explain how the keys combine. Also they should probably mention this is synchonous protocol. I'll divvy up the marks when I see how they coped.

(c) [8 Marks] Shamir's algorithm enables us to share a secret, specifically allowing any n of m members of a group to be able to decode the message. Explain, preferably in a diagram, how key fragments are created, and how we can reconstruct the key from any n of the m fragments.

Slides 7-9 Lecture 6. Drawing some graphs of a line or a parabola and demonstrating finding the y intercept for a polynomial of degree k (line is degree 1, polynomial is degree 2) with k points is impossible if we have but k+1 points it is computable. Keys shares are simply points on the line. I'll divvy up the marks when I see how they coped.

(d) [5 Marks] Show, with the aid of a diagram, how RSA public-private keys can be used to authenticate two parties that can safely obtain, or already have, the other's public key.

Slide 8 Lecture 5. I really want to see nonces in here as well – 2 Marks for that. 1 Mark for the challenge-respone structure, 2 Marks for the correct application of the Public and Private keys.

(e) [5 Marks] Show how, with the aid of a diagram:

i. a digital signature and a digest are used to 'sign' a documents, and
Slide 13, Lecture 6.

ii. how the reciever can check the digital signature without being able to reversing the digest.2
Slide 14, Lecture 6.

Question 3 Application Layer **[30 marks]**

(a) [2 Marks] Define the term 'protocol' as used in computer networking.
Definition: A protocol defines the format and the order of messages exchanged between two or more communicating entities, as well as the actions taken on the transmission and/or receipt of a message or other event.

(b) [3 Marks] Explain, with examples, why the transport layer is considered an Hourglass protocol.
It is a thin protocol neck as in the neck of an hourglass, i.e., instead of a m:n mapping where m applications must be able to transmit over n media, instead we replace the problem with a m:1 and 1:n problem, where the need to deal with different media and different applications is abstracted away on the other side of the transport layer.

(c) [3 Marks] Give three good reasons why layering is a good idea for networking.
- *explicit structure allows identification of the relationships of such a complex system's pieces*
- *modularity eases maintenance and the updating of the system*
- *change of implementation of a layer is transparent to rest of system.*

(d) [4 Marks] Explain the difference between sockets and ports. *Ports are the address space of a protocol resolved within a host. Sockets are a software structure that is bound by the application to a port. A port may have multiple communication channels multiplexed over it, via multiple sockets bound to it.*

(e) [2 Marks] What is SOAP?
The Simple Object Access Protocol is an XML based procotocl used to describe structured typed data.

(f) [4 Marks] What is an RPC/RMI? Include a brief dicussion of how an RPC/RMI is carried out.
Remote Proceedure Call/Remote Method Invocation is a means of executing remote code using local programming semmantics/conventions. A varitey of means can be used to transport RPC/RMI calls, binary etc, through to examples seen in this course of XML-RPC and SOAP. Arguments are marshelled in a stub, sent over the network, unmarshelled in the skeleton/stub at the remote host to suit the remote environment, processed, and then the return values/errors are marshelled and returned to the client and unmarshelled and returned to the calling program.

(g) [4 Marks] Define the difference between a Web-based Service and a Web service.
Web-based services are about services offered through a website, they tend to be vertically integrated. Web services are all about standards for interopterability. Multiple existing webservices can be combined and processed, as in their 306 project and then re-exported as a new 'value-added' service.

(h) DNS

i. [3 Marks] Explain zone delegation in the DNS.
Zones separate the management/responsibility for parts of the namespace. I.e. authority is delegates to InternetNZ for the .nz namespace. They further delegate authority to say vuw, for the .vuw.ac.nz namespace.

ii. [5 Marks] Show, with the aid of diagrams how and iterative DNS query.
Slide 22, lecture 12.

Question 4 Transport Layer **[30 marks]**

(a) [2 Marks] What does it mean for a protocol to be 'connection-less'?
No state about the communication is held in either host stack or the network. Individual packets may take different routes and arrive out of order etc. Example: UDP.

(b) [4 Marks] Discuss why some applications may prefer connection-less protocols to connection oriented procotocls. Use examples to reinforce your explanation.
Connection-less protocols have fewer overheads, and are therefore often faster over the same network. Some applications can benefit from using their own protocols to deal with errors, sequencing etc. Example, VoIP is usually carried out over UDP as packet loss can be tolerated, but extreme packet delay or jitter cannot.

(c) [8 Marks] Explain how TCP deals with duplicate connections requests.
Quite a big answer here. Draw a sequence diagram like L14, Slide 8. Annotate with proper sequence numbers that show how the TCP way handshake rejects the spurious connection. I would also hope for some comment about how the 2nd connection request happened – i.e. store and forward network, with timeouts and resends.

(d) [8 Marks] Explain TCP's mechanism for flow control. Use diagrams to show how the receive window operates and be sure to detail how the receive window information is communicated back to the sender.
L14, S13-15.

(e) [8 Marks] Explain TCP's mechanism for conjestion control. Be sure to include a brief discussion on slow start, fast retransmit and fairness.
All the good stuff like Reno and Tahoe etc from L15, S19-22.

Question 4 Network Layer and IP Addressing **[35 marks]**

(a) [10 marks] Consider a datagram network using 8-bit host addresses. Suppose a router uses longest prefix matching and has the following forwarding table:

Prefix Match	Interface
00	0
010	1
011	2
10	2
11	3

For each of the four interfaces, give the associated range of destination host addresses and the number of addresses in the range (write your answer in the table below).

Answer:

Destination Address Range	Interface	No. of Addresses
through	0	
through	1	
through	2	
through	2	
through	3	

(b) [14 marks] Consider the following topology, which has six subnets (A, B, C, D, E and F). Suppose all addresses for the host and router interfaces MUST be allocated from 214.97.254/23. Assign network addresses to each of the six subnets with the following requirements:

1. Subnet A should have enough addresses to support 250 interfaces.
2. Subnet B should have enough addresses to support EXACTLY 120 interfaces.
3. Subnet C should have enough addresses to support 120 interfaces.
4. Subnets D, E and F should each be able to support two interfaces.

For each subnet, the assignment should take the form a.b.c.d/x or a.b.c.d/x – e.f.g.h/y (write your answer in the table below).

Subnet	**Address**
A	
B	
C	
D	
E	
F	

(f) [3 marks] What is the deference between CIDR (Classless Interdomain Routing) and Classful Addressing?

(g) [3 marks] What does DHCP do?

(h) [5 marks] What is NAT traversal problem and how to address this problem using UPnP (Universal Plug and Play)?

Question 6 Routing and Mobile Networks **[25 marks]**

(a) [17 marks] Consider the network shown below, and assume that each node initially knows the link costs to each of its neighbours. Compute **the distance table at Node Z** after the initialisation step and after each iteration of a synchronous version of the distance-vector algorithm - nodes exchange cost information in a synchronous manner (write your answer in the tables below).

Answer:

		Cost to				
		U	V	X	Y	Z
From	V					
	X					
	Z					

		Cost to				
		U	V	X	Y	Z
From	V					
	X					
	Z					

		Cost to				
		U	V	X	Y	Z
From	V					
	X					
	Z					

		Cost to				
		U	V	X	Y	Z
From	V					
	X					
	Z					

		Cost to				
		U	V	X	Y	Z
From	V					
	X					
	Z					

(b) [3 marks] In Mobile IP, what is the difference between a permanent address and a care-of address? Who assigns a care-of address?

(c) [5 marks] What are the purposes of the HLR and VLR in GSM networks? What elements in Mobile IP are similar to the HLR and VLR?

* * * * * * * * * * * * * * * * * * *